1, P

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/974,705	10/10/2001	Marco Macchetti	01AG17653537	7872

27975 7590 06/07/2006

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST P.A.
1401 CITRUS CENTER 255 SOUTH ORANGE AVENUE
P.O. BOX 3791
ORLANDO, FL 32802-3791

EXAMINER	
COLIN, CARL G	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 06/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/974,705	MACCHETTI ET AL.	
	Examin r	Art Unit	
	Carl Colin	2136	

-- Th MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 April 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/14/2006 has been entered.

Response to Arguments

2. In response to communications filed on 3/24/2006, applicant amends claims 21, 25, 31, 44, the following claims 21-47 are presented for examination.

2.1 In response to communications filed on 3/24/2006, Applicant has not addressed the 112th rejection with respect to claim 25; the amendment does not clarify how the performing step is done. The claimed limitation is not definite, the claim recites performing a round once ... it seems that there has been a typographical error once should have been read --on-- as the claim does not recite on what the performing is done (the specification, page 8, describes transformation is carried out on a non-transposed state) applicant did not overcome the rejection in the previous Office action when amending claim 25 by adding the word "occurs". Applicant now adds other limitations that are still inconsistent with the specification.

2.2 Applicant's remarks, pages 11-16, filed on 3/14/2006, with respect to the rejection of claims 21-47 have been fully considered but they are not persuasive. Applicant has amended the independent claims to recite transposing each of the rows and columns instead of transposing rows and columns Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made. Further, they do not show how the amendments avoid such references or objections. Applicant mentions there is nothing in the disclosure of suggesting transposing rows and columns of a state array (matrix). Examiner respectfully disagrees. Ohkuma discloses a non-transposed matrix (state array) into a transposed matrix (state array) wherein a matrix obtained by substituting rows and substituting columns and transposing in a matrix (state array) may be used. As interpreted by examiner the transposing is performed by substituting rows and substituting columns to obtain a transposed MDS matrix (state array) that meets the recitation of transposing each row and column of the state array to form a transposed state array (paragraphs 261-271 see figure 3). Therefore, claims 21-47 are still rejected in view of Ohkuma.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 21, 31, and 44 and the intervening claims are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains

subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The specification fails to explicitly disclose transposing each of the rows and columns of the state array to form a transposed state array.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claim 25 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4.1 Regarding claim 25, the recitation "wherein performing comprises performing at least one transformation round once the non-transposed state array in at least one of the plurality of transformation rounds occurs" renders the claim(s) indefinite because the claim(s) include(s) elements not actually disclosed (those encompassed by " performing at least one transformation round once a non-transposed state array occurs"), thereby rendering the scope of the claim(s) unascertainable. Also, there is lack of consistency of the claim with the original disclosure as there is no mention in the original disclosure of making a determination for non-transposed state array in at least one of the plurality of transformation rounds and there is no performing transformation once the non-transposed state occurs in the original disclosure.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.1 **Claims 21-47** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US 2001/0024502 to **Ohkuma et al**.

5.2 **As per claims 21, 26, 31, and 44, Ohkuma et al** substantially teaches a device for converting data between an unencrypted format and an encrypted format, the device comprising: at least one register for storing the data in the form of bit words (see figure 10); and a circuit for performing a plurality of transformation rounds (see paragraph 92), each transformation round comprising applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array (page 12, paragraphs 261-274 and figure 3), and **Ohkuma et al** discloses that a matrix obtained by substituting rows and substituting columns and transposing the rows and columns in another matrix (state array) may be used. As interpreted by examiner the transposing is performed by substituting rows and substituting columns to obtain a

transposed MDS matrix (state array) that meets the recitation of transposing each row and column of the state array to form a transposed state array because the transposition is applied to all the values (see paragraphs 261-271 see figure 3); for instance, in figure 3, to obtain y, a transformation is performed to obtain a transposed state of the matrix (paragraph 270 states executing transformation by means of a matrix) therefore, **Ohkuma et al** discloses transposing each of the rows and columns of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array. **Ohkuma et al** in another embodiment discloses applying key scheduling on a higher level MDS matrix, for example (page 13, paragraphs 306-315). Although **Ohkuma et al** does not disclose the same architecture as in applicant's disclosure, **Ohkuma et al** discloses different arrangements in the disclosure that read on the claimed language as claimed. To shift location of parts requires routine skill in the art-*In re Japikse* 86 USPQ 70 (CCPA 1950). And as suggested by **Ohkuma et al** page 15, paragraphs 352-354, replacing, omitting, some components of the exemplified arrangement and adding other functions or combining them to the exemplified arrangement would require routine skill in the art and therefore, one of ordinary skill in the art it would have been motivated to combine, add, omit, replace components that achieve same or similar functions to those disclosed by **Ohkuma et al** in the exemplified arrangement so as to reach a design goal such as higher speed processing; multiprocessor may be used to execute parallel processed thus achieving high speed processing as suggested by **Ohkuma et al** (see paragraph 133).

As per claims 22 and **32**, **Ohkuma et al** discloses the limitation of wherein said at least one register stores bit words as 8-bit words (page 6, paragraph 128).

As per claims 23 and **33**, **Ohkuma et al** discloses the limitation of wherein said circuit operates on a state array comprising a 4x4 matrix of bit words (page 6, paragraph 128).

As per claims 24 and **34**, **Ohkuma et al** discloses the limitation of said circuit in performing a plurality of transformation rounds performs at least 10 transformation rounds (page 4, paragraph 92).

As per claim 25, **Ohkuma et al** discloses performing in at least one stage or round, non-transposed matrix (state array) by executing transformation by means of a matrix (paragraphs 268-270) as shown in figure 30 see detailed explanation. Performing at least one round on a non-transposed state array is well known as disclosed in Rijndael cipher algorithm. (See also page 13, paragraph 305, and prior art figure 4 of Applicant's disclosure).

As per claim 27, **Ohkuma et al** discloses the limitation of wherein the at least one round key is transposed (see figure 3 and figure 6 and page 5, paragraph 109).

As per claims 28-30, **Ohkuma et al** discloses the limitation of adding code to transpose the at least one round key wherein the at least one round key comprises a plurality of round keys, each corresponding to a respective transformation round and being applied according to a round

key schedule wherein the round key schedule comprises a transposed round key schedule (pages 4-5, paragraphs 90-98 and page 5, paragraph 109).

As per claims 35-36, and **45**, **Ohkuma et al** discloses that the invention can be performed by any number of modules and any combination of bits that meets the recitation of wherein said circuit comprises at least one S-box processing module, said at least one S-box processing module operating on a group of bit words defining a cell of a column of the state array and each of the plurality of S-box modules operating on a corresponding cell of a column of the state array (page 3, paragraphs 62-65).

As per claim 37, **Ohkuma et al** discloses the limitation of wherein the column of the state array comprises four cells (page 4, paragraph 92).

As per claims 38-39 and **46-47**, **Ohkuma et al** discloses that the invention can be performed by any number of modules and any combination of bits wherein the circuit further comprises a plurality of shift column modules, (page 3, paragraphs 62-65); and further discloses shift up can be performed (page 5, paragraph 117); column mix is also a well known process as disclosed in Rijndael cipher algorithm (page 1, paragraph 5 and page 4, paragraph 87) that meets the recitation of each of said plurality of shift column modules to perform a column shift operation on a column of the state array and the limitation of wherein a column shift operation performed by each of said plurality of shift column modules generates shift column data, and

wherein said circuit further comprises a single mix column module to perform column mix operations on shift column data

As per claims 40-43, **Ohkuma et al** discloses an encryption and decryption apparatus that meets the recitation of encoder for converting data from an unencrypted data format to an encrypted data format and a decoder for converting data from an encrypted data format to an unencrypted data format (page 15, paragraph 343-349). **Ohkuma et al** further discloses an encryption and decryption apparatus formed as a semiconductor device that meets the recitation of embedded system for use in a smart card (page 15, paragraph 343-349).

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin

Patent Examiner

May 31, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100